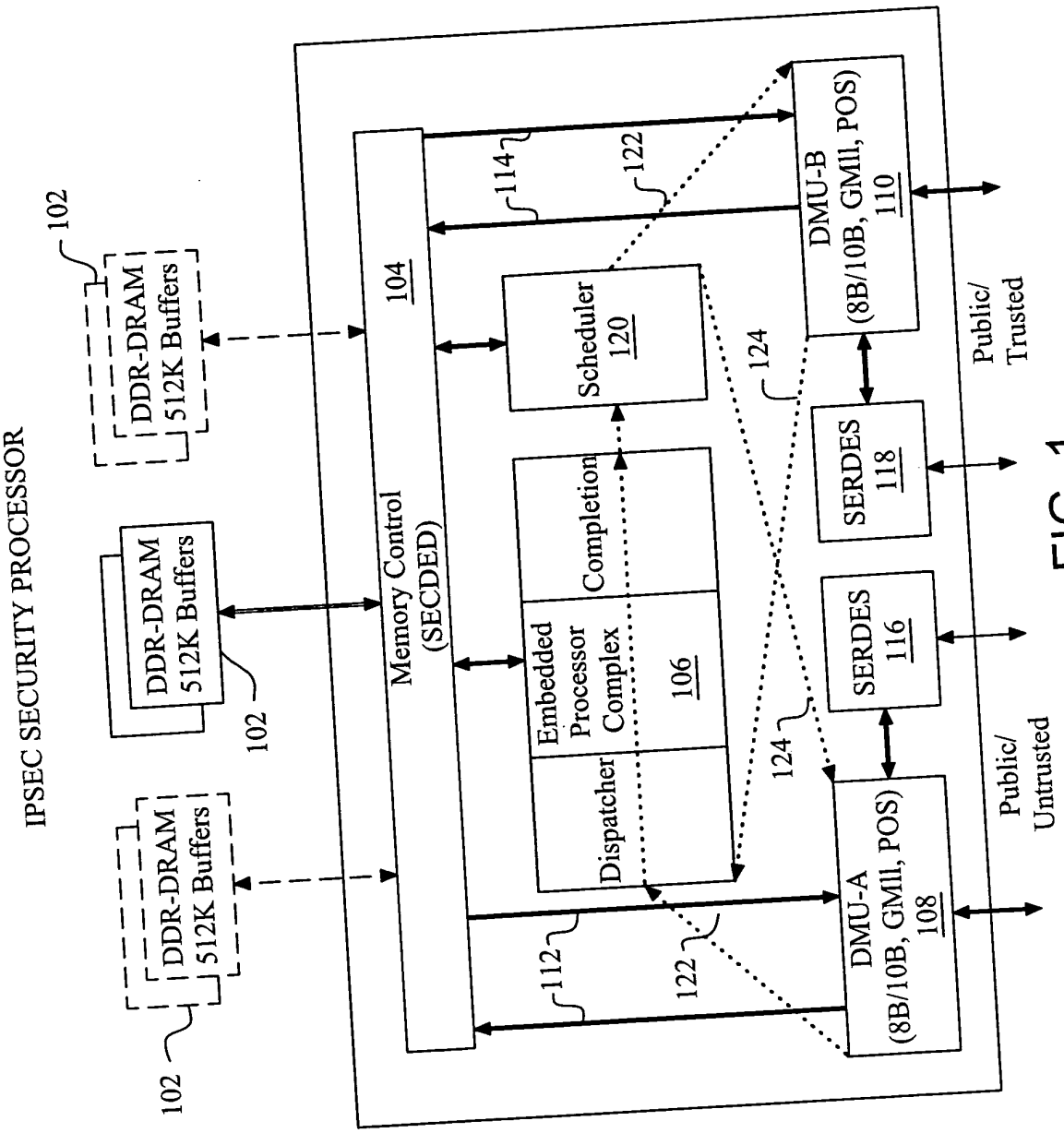
IPSEC SECURITY PROCESSOR
102
DDR-DRAM
512K Buffers
102
DDR-DRAM
512K Buffers
102
DDR-DRAM
512K Buffers
Memory Control
(SECDED)
104
114
122
DMU-B
(8B/10B, GMII, POS)
110
Scheduler
120
124
Embedded
Processor
Complex
106
Completion
Dispatcher
SERDES
118
SERDES
116
Public/
Trusted
Public/
Untrusted
112
122
124
DMU-A
(8B/10B, GMII, POS)
108

FIG. 1

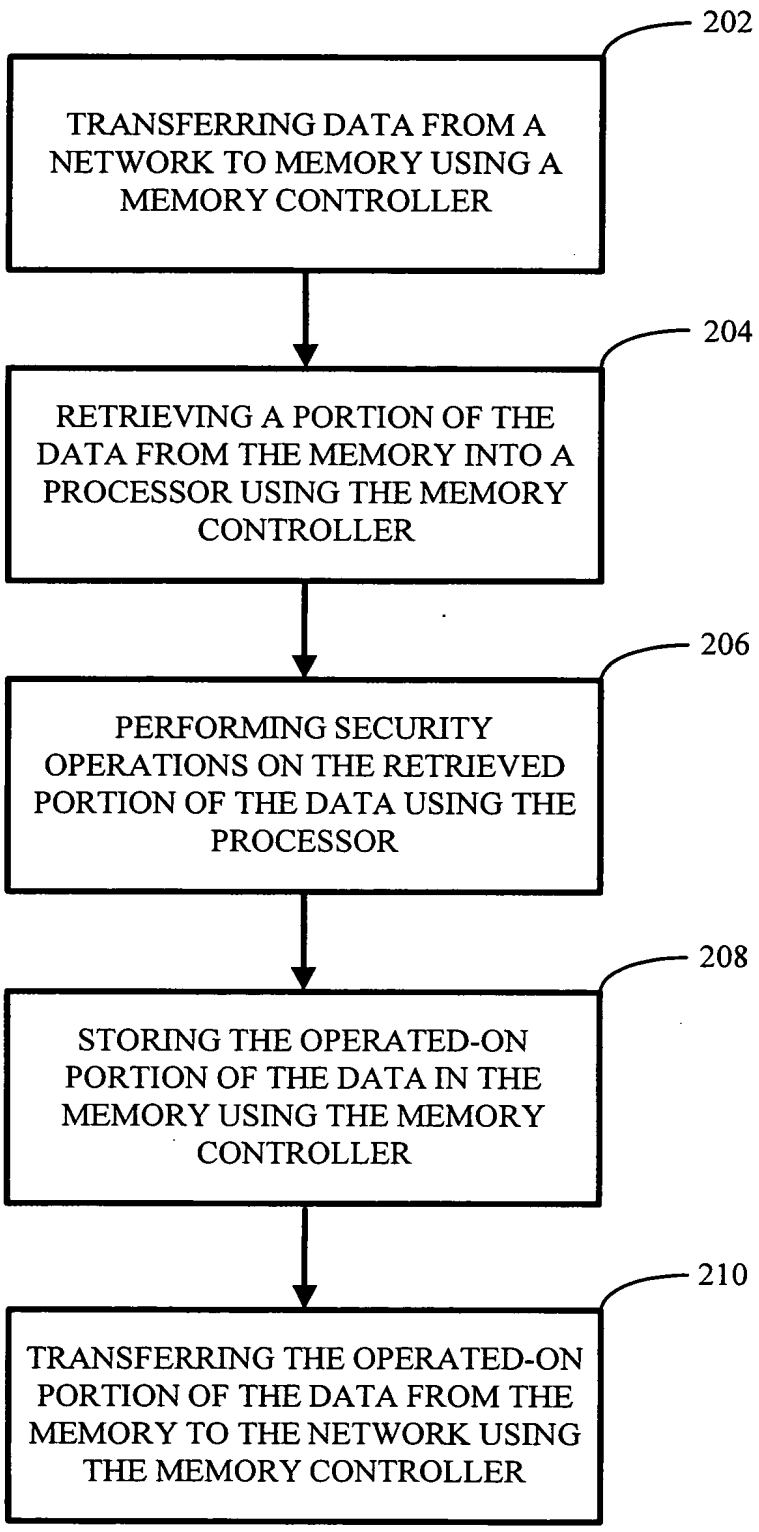
202
TRANSFERRING DATA FROM A NETWORK TO MEMORY USING A MEMORY CONTROLLER
204
RETRIEVING A PORTION OF THE DATA FROM THE MEMORY INTO A PROCESSOR USING THE MEMORY CONTROLLER
206
PERFORMING SECURITY OPERATIONS ON THE RETRIEVED PORTION OF THE DATA USING THE PROCESSOR
208
STORING THE OPERATED-ON PORTION OF THE DATA IN THE MEMORY USING THE MEMORY CONTROLLER
210
TRANSFERRING THE OPERATED-ON PORTION OF THE DATA FROM THE MEMORY TO THE NETWORK USING THE MEMORY CONTROLLER

FIG. 2

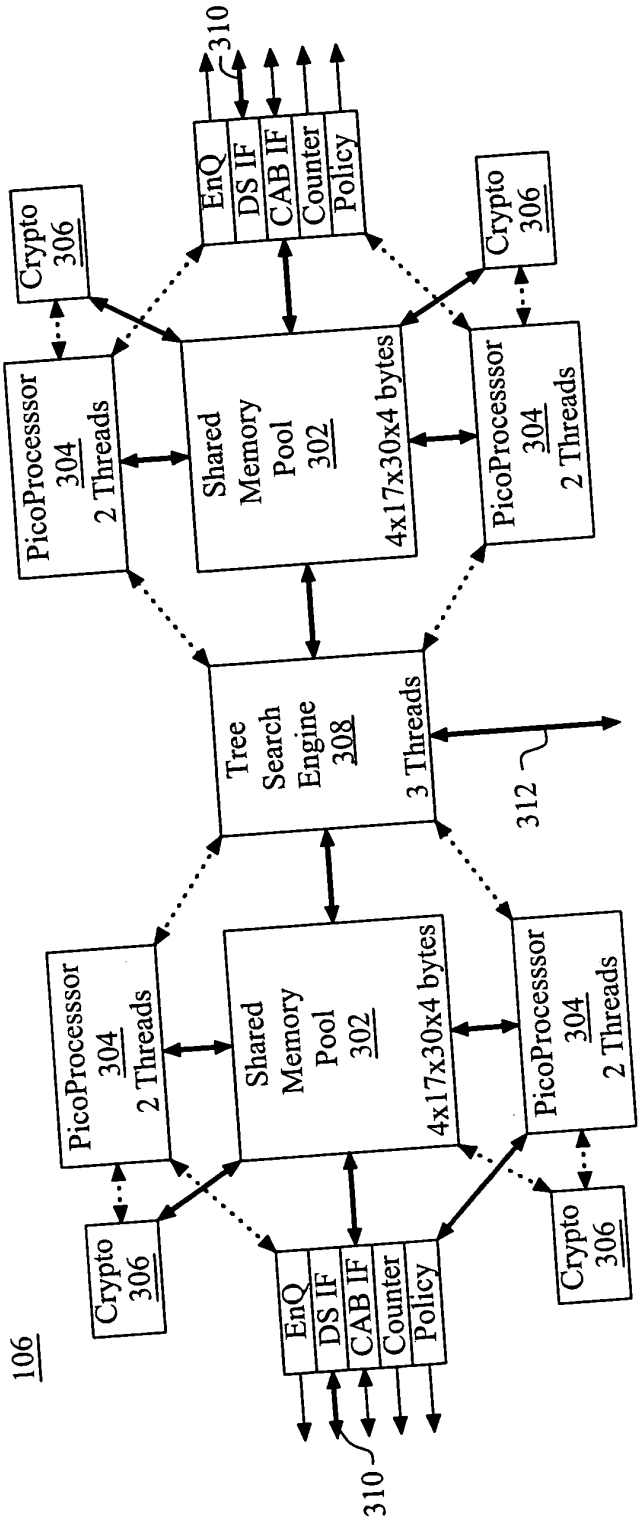
EMBEDDED PROCESSOR COMPLEX
106
310
EnQ
DS IF
CAB IF
Counter
Policy
Crypto 306
PicoProcessor 304 2 Threads
Shared Memory Pool 302
4x17x30x4 bytes
Tree Search Engine 308
3 Threads
312
310

FIG. 3

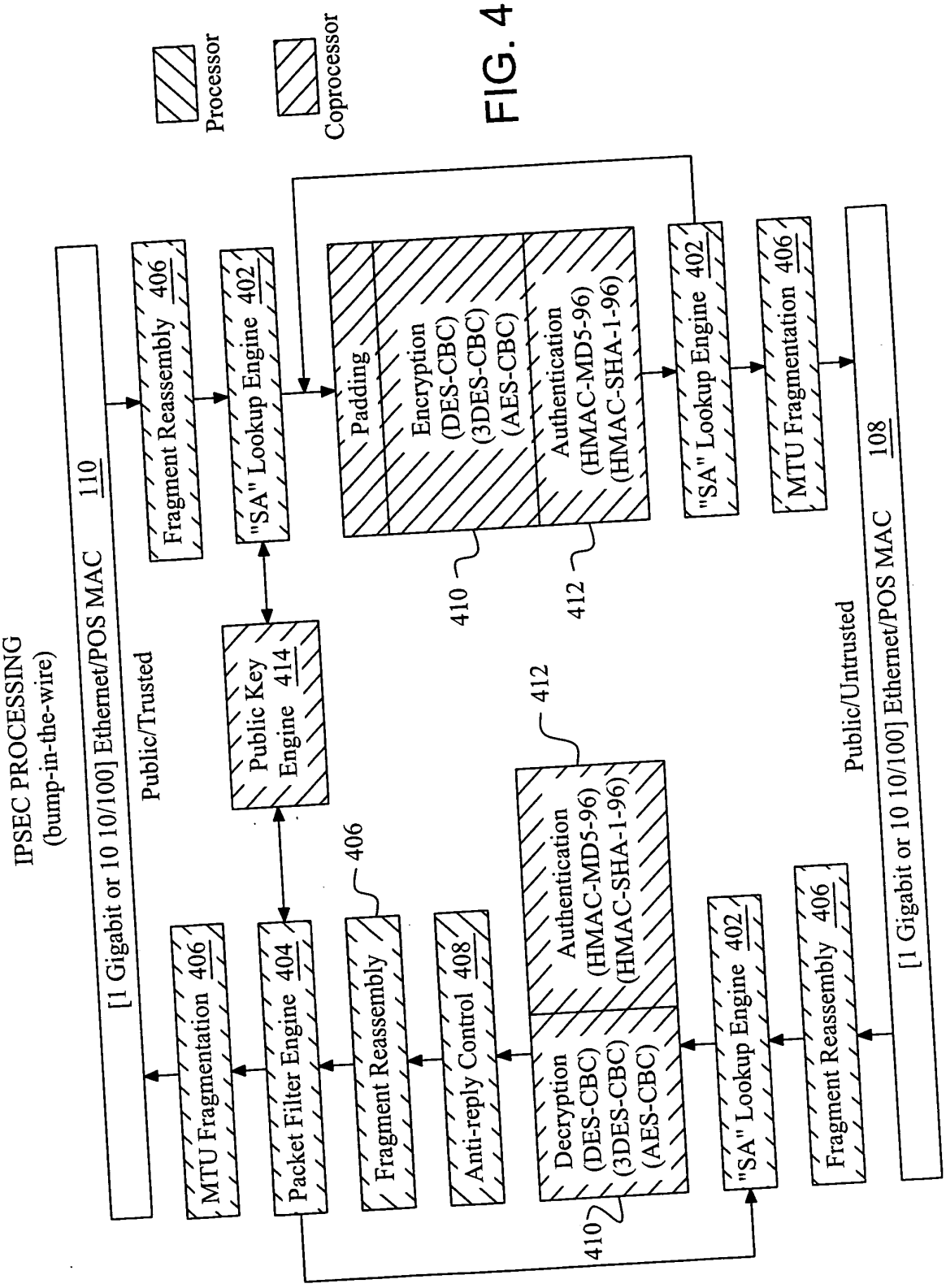
IPSEC PROCESSING
(bump-in-the-wire)
[1 Gigabit or 10 10/100] Ethernet/POS MAC 110
Public/Trusted
MTU Fragmentation 406
Packet Filter Engine 404
Fragment Reassembly 406
Anti-reply Control 408
Decryption (DES-CBC) (3DES-CBC) (AES-CBC)
Authentication (HMAC-MD5-96) (HMAC-SHA-1-96)
"SA" Lookup Engine 402
Fragment Reassembly 406
Public Key Engine 414
Fragment Reassembly 406
"SA" Lookup Engine 402
Padding
Encryption (DES-CBC) (3DES-CBC) (AES-CBC)
Authentication (HMAC-MD5-96) (HMAC-SHA-1-96)
"SA" Lookup Engine 402
MTU Fragmentation 406
Public/Untrusted
[1 Gigabit or 10 10/100] Ethernet/POS MAC 108
410
412
412
410
406
Processor
Coprocessor

FIG. 4

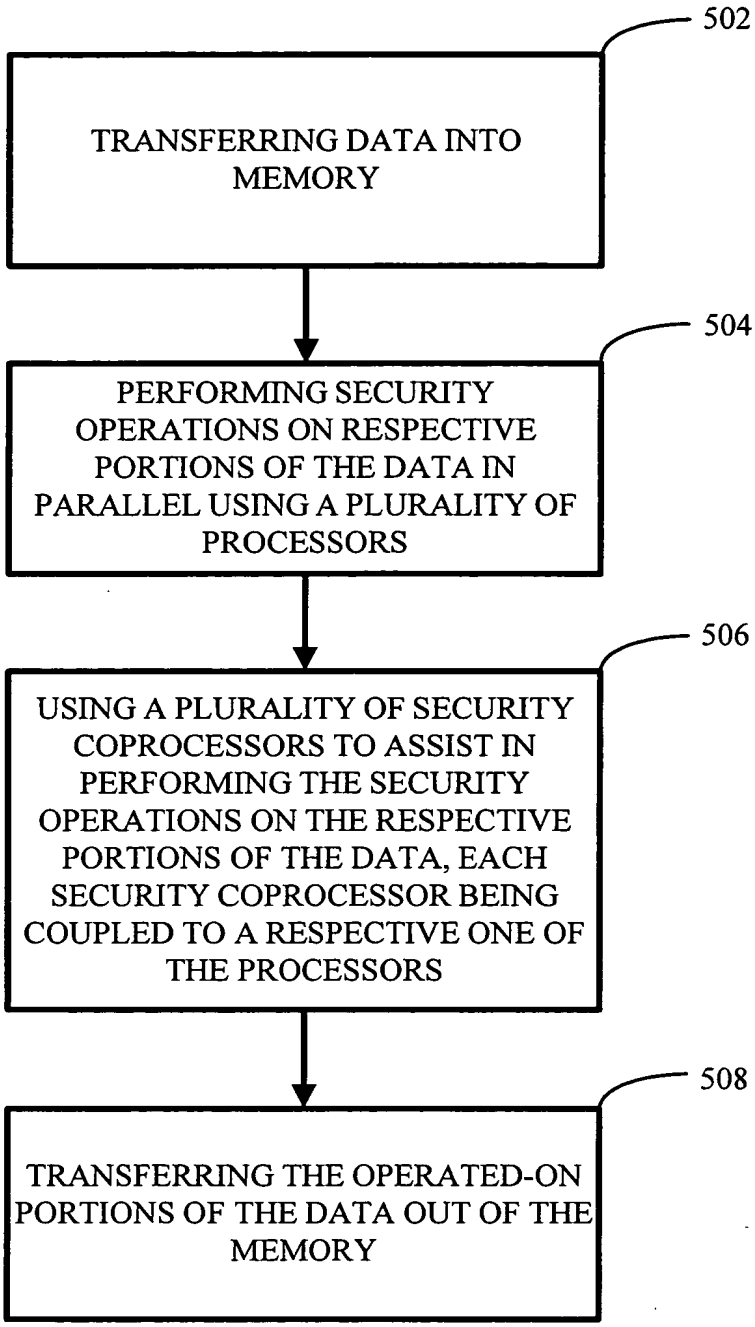
502
TRANSFERRING DATA INTO MEMORY
504
PERFORMING SECURITY OPERATIONS ON RESPECTIVE PORTIONS OF THE DATA IN PARALLEL USING A PLURALITY OF PROCESSORS
506
USING A PLURALITY OF SECURITY COPROCESSORS TO ASSIST IN PERFORMING THE SECURITY OPERATIONS ON THE RESPECTIVE PORTIONS OF THE DATA, EACH SECURITY COPROCESSOR BEING COUPLED TO A RESPECTIVE ONE OF THE PROCESSORS
508
TRANSFERRING THE OPERATED-ON PORTIONS OF THE DATA OUT OF THE MEMORY

FIG. 5

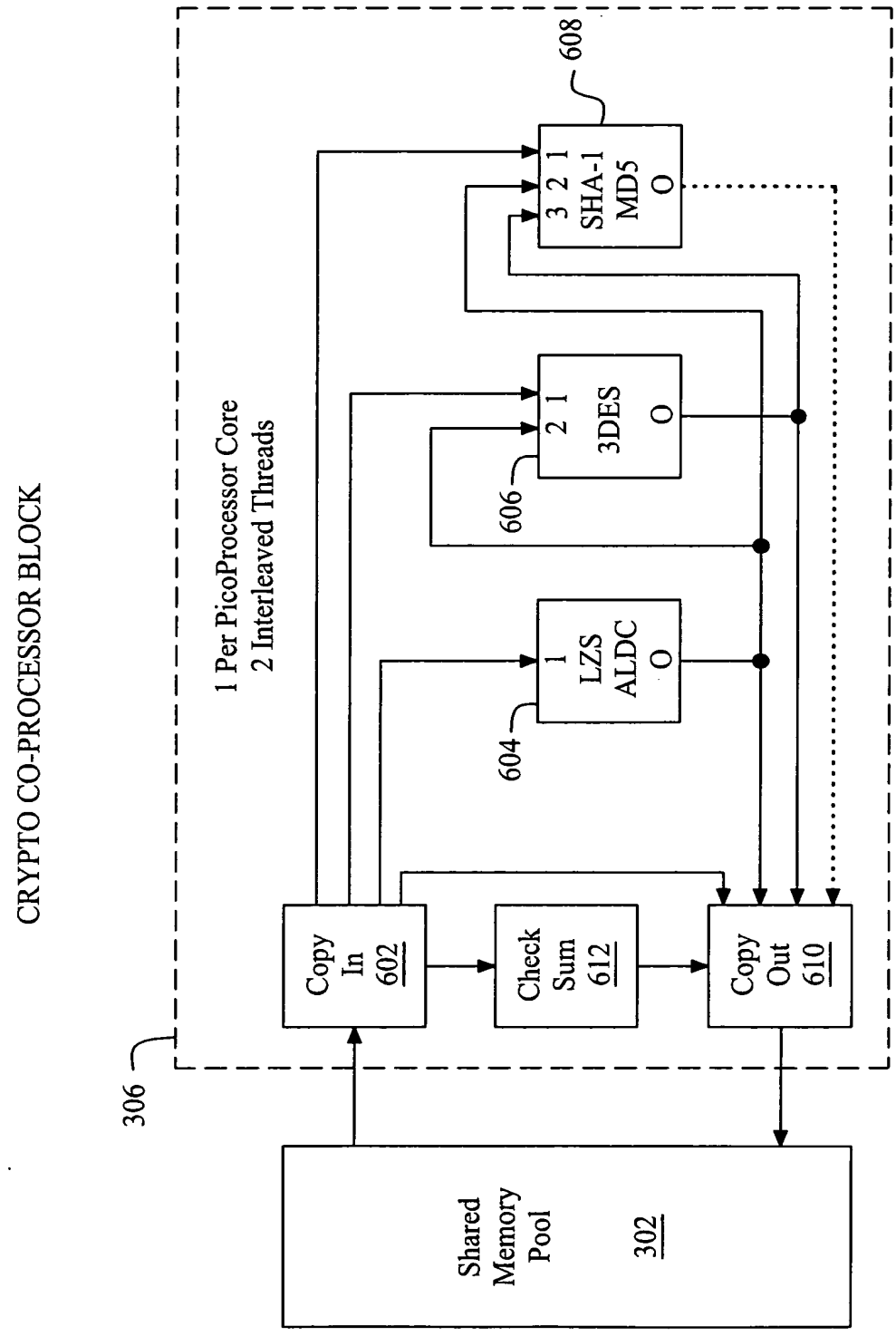
CRYPTO CO-PROCESSOR BLOCK
306
1 Per PicoProcessor Core
2 Interleaved Threads
608
3 2 1
SHA-1
MD5
0
606
2 1
3DES
0
604
1
LZS
ALDC
0
Copy
In
602
Check
Sum
612
Copy
Out
610
Shared
Memory
Pool
302

FIG. 6

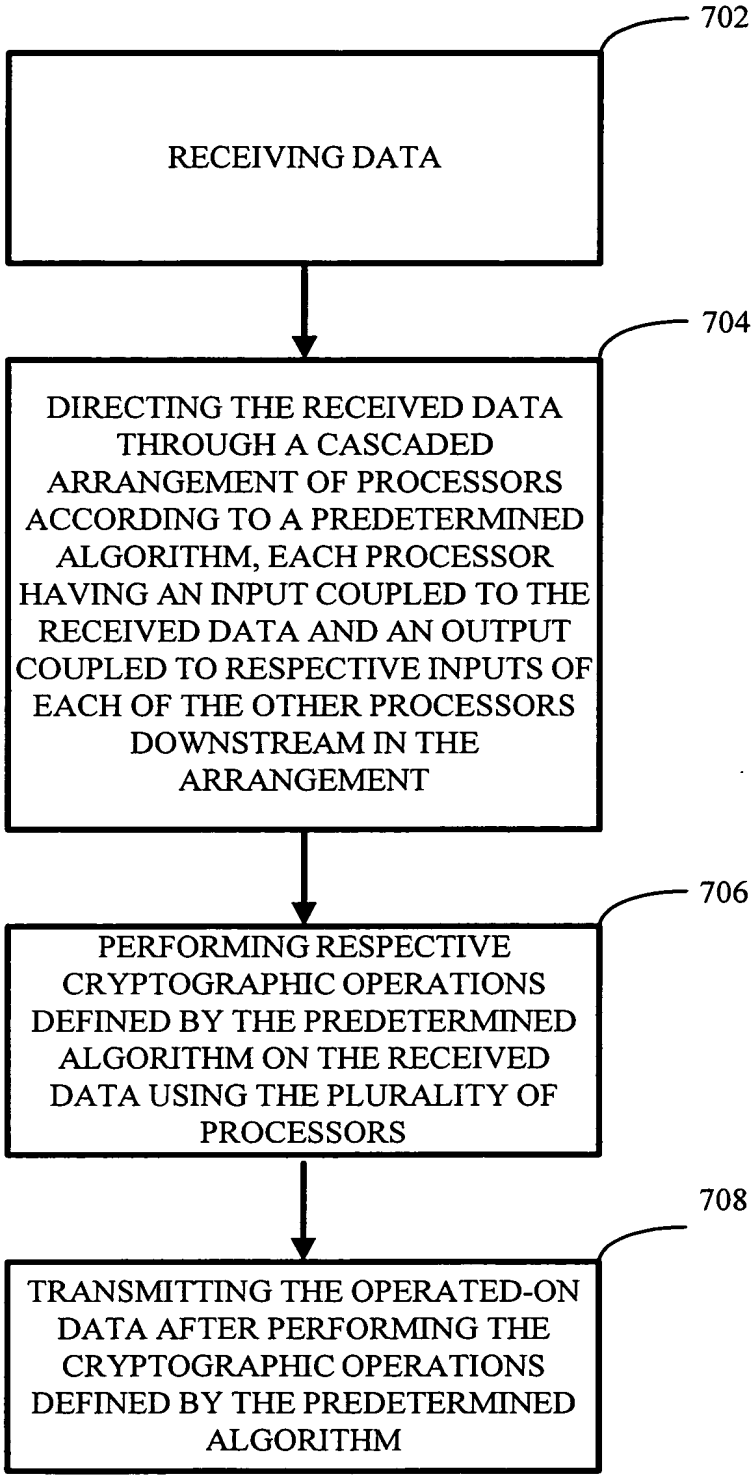
702
RECEIVING DATA
704
DIRECTING THE RECEIVED DATA THROUGH A CASCADED ARRANGEMENT OF PROCESSORS ACCORDING TO A PREDETERMINED ALGORITHM, EACH PROCESSOR HAVING AN INPUT COUPLED TO THE RECEIVED DATA AND AN OUTPUT COUPLED TO RESPECTIVE INPUTS OF EACH OF THE OTHER PROCESSORS DOWNSTREAM IN THE ARRANGEMENT
706
PERFORMING RESPECTIVE CRYPTOGRAPHIC OPERATIONS DEFINED BY THE PREDETERMINED ALGORITHM ON THE RECEIVED DATA USING THE PLURALITY OF PROCESSORS
708
TRANSMITTING THE OPERATED-ON DATA AFTER PERFORMING THE CRYPTOGRAPHIC OPERATIONS DEFINED BY THE PREDETERMINED ALGORITHM

FIG. 7